Deployment, Installation, Back-Out, and Rollback Guide

Medical Care Collection Fund (MCCF) Electronic Data Interchange (EDI) Transaction Applications Suite (TAS) Phase 2

eInsurance IB*2.0*659

April 2020

Document Version 1.3

Department of Veterans Affairs

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
March 2020	1.3	Added test sites – IOC Exit	Darlene White
Feb. 14, 2020	1.2	Updates for additional prerequisites (IB*602 & IB*623) and small change in scope as we are now addressing two service tickets for VA. This version of this document is for the MOU needed for adding a new IOC site to our testing efforts.	Darlene White
Jan 21, 2020	1.1	Updates for Feedback – IOC Entry	Darlene White
Dec 18, 2019	1.0	Initial document – IOC Entry	Vito D’Amico
Oct. 2019	Draft	Draft Version	Vito D’Amico

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all of these activities. Its purpose is to provide clients, stakeholders, and support personnel a smooth transition to the new product or software. This document should be structured to reflect the application of these procedures to either a single site or to multiple sites.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

Table of Tables

1 Introduction

This document describes how to deploy and install the IB*2.0*659 patch and how to back-out the product and rollback to a previous version or data set.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom IB*2.0*659 will be deployed and installed, as well as how the patches are to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2 Dependencies

The following patches must be installed **before** IB*2.0*659:

- IB*2.0*517
- IB*2.0*521
- IB*2.0*602
- IB*2.0*623
- IB*2.0*631

1.3 Constraints

This patch is intended for a fully patched VistA system.

2 Roles and Responsibilities

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	VA OI&T, VA OI&T Health Services Portfolio& PMO	Deployment	Plan and schedule deployment (including orchestration with vendors)	Planning
2	Local VAMC and CPAC processes	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Planning

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
3	Field Testing (Initial Operating Capability (IOC)), Health Services Portfolio Testing & VIP Release Agent Approval	Deployment	Test for operational readiness	Testing
4	Health Services Portfolio and Field Operations	Deployment	Execute deployment	Deployment
5	Individual Veterans Affairs Medical Centers (VAMCs)	Installation	Plan and schedule installation	Deployment
6	VIP Release Agent	Installation	Ensure authority to operate and that certificate authority security documentation is in place	Deployment
7	N/A for this patch as we are using only the existing VistA system	Installation	Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes	N/A
8	VA's eBusiness team	Installation	Coordinate training	Deployment
9	VIP release Agent, Health Services Portfolio & the development team	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	Deployment
10	No changes to current process – we are using the existing VistA system	Post Deployment	Hardware, Software and System Support	Warranty

3 Deployment

The deployment is planned as a national rollout.

This section provides the schedule and milestones for the deployment.

3.1 Timeline

The deployment and installation is scheduled to run for 30 days, as depicted in the master deployment schedule[1].

[1] Project schedule (right click and select open hyperlink to access)
MCCF TAS IMS Schedule.zip

3.2 Site Readiness Assessment

This section discusses the locations that will receive the IB*2.0*659 deployment.

3.2.1 Deployment Topology (Targeted Architecture)

This patch IB*2.0*659 is to be nationally released to all VAMCs.

3.2.2 Site Information (Locations, Deployment Recipients)

The test sites for IOC testing are:

- Birmingham, AL
- Las Vegas, NV
- Miami, FL
- San Antonio, TX

Upon national release all VAMCs are expected to install this patch within the compliance dates.

3.2.3 Site Preparation

The following table describes preparation required by the site prior to deployment.

Table 2: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
N/A	N/A	N/A	N/A	N/A

3.3 Resources

3.3.1 Facility Specifics

The following table lists facility-specific features required for deployment.

Table 3: Facility-Specific Features

Site	Space/Room	Features Needed	Other
N/A	N/A	N/A	N/A

3.3.2 Hardware

The following table describes hardware specifications required at each site prior to deployment.

Table 4: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Existing VistA system	N/A	N/A	N/A	N/A	N/A

Please see the Roles and Responsibilities table in Section 2 for details about who is responsible for preparing the site to meet these hardware specifications.

3.3.3 Software

The following table describes software specifications required at each site prior to deployment.

Table 5: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
Fully patched Integrated Billing package within VistA	N/A	2.0	N/A	N/A	N/A
IB*2.0*517	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*521	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*602	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*623	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*631	N/A	Nationally released version	N/A	N/A	N/A

Please see the Roles and Responsibilities table in Section 2 above for details about who is responsible for preparing the site to meet these software specifications.

3.3.4 Communications

The sites that are participating in field testing (IOC) will use the “Patch Tracking” message in Outlook to communicate with the eBusiness eInsurance sub-team, the developers, and product support personnel.

3.3.4.1 Deployment/Installation/Back-Out Checklist

The Release Management team will deploy the patch IB*2.0*659, which is tracked in the National Patch Module (NPM) in Forum, nationally to all VAMCs. Forum automatically tracks the patches as they are installed in the different VAMC production systems. One can run a report in Forum to identify when and by whom the patch was installed in the VistA production at each site. A report can also be run to identify which sites have not currently installed the patch in their VistA production systems. Therefore, this information does not need to be manually tracked in the chart below.

Table 6: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual who completed task
Deploy	N/A	N/A	N/A
Install	N/A	N/A	N/A
Back-Out	N/A	N/A	N/A

4 Installation

4.1 Pre-installation and System Requirements

IB*2.0*659, a patch to the existing VistA Integrated Billing 2.0 package, is installable on a fully patched M(UMPS) VistA system and operates on top of the VistA environment provided by the VistA infrastructure packages. The latter provides utilities which communicate with the underlying operating system and hardware, providing Integrated Billing independence from variations in hardware and operating system.

4.2 Platform Installation and Preparation

Refer to the IB*2.0*659 documentation on the National Patch Module (NPM) on Forum for the detailed installation instructions. These instructions will include any pre installation steps if applicable.

4.3 Download and Extract Files

Refer to the IB*2.0*659 documentation on the NPM to find the location of related documentation that can be downloaded. IB*2.0*659 will be transmitted via a PackMan message and can be pulled from the NPM. It is not a host file, and therefore does not need to be downloaded separately.

4.4 Database Creation

IB*2.0*659 does modify the data in the VistA database. Two new eIV site parameters have been created. These two new fields are: MEDICARE FRESHNESS DAYS (#350.9, 51.32) and MANILA EIV ENABLED (#350.9, 51.33).

4.5 Installation Scripts

No installation scripts are needed for IB*2.0*659 installation.

4.6 Cron Scripts

No Cron scripts are needed for IB*2.0*659 installation.

4.7 Access Requirements and Skills Needed for the Installation

The following staff need access to the PackMan message containing the IB*2.0*659 patch or Forum's NPM in order to download the nationally released IB*2.0*659 patch. The software is to be installed by the sites or regions designated: VA OI&T IT OPERATIONS SERVICE, Enterprise Service Lines, and/or VistA Applications Division[2].

4.8 Installation Procedure

Refer to the IB*2.0*659 documentation on the NPM for the detailed installation instructions.

4.9 Installation Verification Procedure

Refer to the IB*2.0*659 documentation on the NPM for detailed installation instructions. These instructions include any post installation steps if applicable.

4.10 System Configuration

No system configuration changes are required for this patch.

4.11 Database Tuning

No reconfiguration of the VistA database, memory allocations or other resources is necessary.

5 Back-Out Procedure

Back-Out pertains to a return to the last known valid instance of operational software and platform settings.

5.1 Back-Out Strategy

Although it is unlikely, due to care in collecting, elaborating, and designing approved user stories, followed by multiple testing stages (Developer Unit Testing, Component Integration Testing, SQA Testing, and User Acceptance Testing), a back-out decision due to major issues with this patch could occur during site Mirror Testing, Site Production Testing or after National Release to the field (VAMCs). The best strategy is dependent on the stage during which the decision is made.

If during Mirror testing or Site Production Testing, a new version of a defect correcting test patch is produced, retested and successfully passes development team testing, it would be resubmitted to the site for testing. If the patch produced catastrophic problems, a new version of the patch can be used to restore the build components to their pre-patch condition.

If the defect(s) were not discovered until after national release but during the designated support period, a new patch will be entered into the National Patch Module on Forum and go through all the necessary milestone reviews etc., as a patch for a patch. It is up to VA OI&T and product support whether this new patch would be defined as an emergency patch or not. This new patch could be used to address specific

[2] "Enterprise service lines, VAD" for short. Formerly known as the IRM (Information Resources Management) or IT support.

issues pertaining to the original patch or could be used to restore the build components to their original pre-patch condition.

After the support period, the VistA Maintenance Program would produce the new patch, either to correct the defective components or to back-out the patch.

5.2 Back-Out Considerations

It is necessary to determine if a wholesale back-out of the patch IB*2.0*659 is needed or if a better course of action is to correct through a new version of the patch (if prior to national release) or through a subsequent patch aimed at specific areas modified or affected by the original patch (after national release). A wholesale back-out of the patch will still require a new version (if prior to national release) or a subsequent patch (after national release). If the back-out is post-release of this patch IB*2.0*659, this patch should be assigned status of “Entered in Error” in Forum’s NPM.

5.2.1 Load Testing

N/A. The back-out process if necessary is executed at normal, rather than raised job priority, and is expected to have no significant effect on total system performance. Subsequent to the reversion, the performance demands on the system would be unchanged.

5.2.2 User Acceptance Testing

1. VistA has been modified so the Coordination of Benefits (COB) column will display as P (for Primary), S (for Secondary), T (for Tertiary) and UNK (for Unknown) when the user scrolls right on the screen for the following options:
    - Patient Insurance Info View/Edit [IBCN PATIENT INSURANCE] (summary section)
    - View Patient Insurance [IBCN VIEW PATIENT INSURANCE]
    - Claims Tracking Edit [IBT EDIT BI TRACKING ENTRY]
    - Claims Tracking Edit [IBT EDIT HR TRACKING ENTRY]
    - Claims Tracking Edit [IBT EDIT IR TRACKING ENTRY]
    - Claims Tracking Edit [IBT EDIT TRACKING ENTRY]
    - Third Party Joint Inquiry [IBJ THIRD PARTY JOINT INQUIRY]

2. VistA has been modified to prevent Manila OC, PI (Site #358) from creating and sending eIV messages to FSC. This required the creation of a new eIV site parameter called "MANILA EIV ENABLED" (#350.9,51.33) under the Insurance Verification section of the MCCR Site Parameter Display/Edit [IBJ MCCR SITE PARAMETERS] option. This field is set to a default value of "N" for NO.

3. VistA has been modified to change the eIV Appointment extract frequency from 180 days to 365 days for Medicare policies A, B, C and D. This required the creation of a new eIV site parameter called "MEDICARE FRESHNESS DAYS" (#350.9,51.32) under the Insurance Verification section of the MCCR Site Parameter Display/Edit [IBJ MCCR SITE PARAMETERS] option. This field is set to a default value of 365 days.

4. VistA has been modified to include the new MEDICARE FRESHNESS DAYS (#350.9,51.32) eIV site parameter in the eIV Daily Registration HL7 message.

5. VistA has been modified to automatically check via the eIV Nightly Process [IBCNE IIV BATCH PROCESS] each night (except on Sundays) to determine whether a site's "IIV EC" HL7 Logical

Link is up and running without any stuck messages. If "IIV EC" is down or a stuck message is encountered, an email alert will be sent to the “VHAeInsuranceRapidResponse@va.gov" mail group indicating that there is an issue with the "IIV EC" link.

6. VistA has been modified so that the eIV Response Report [IBCNE IIV RESPONSE REPORT] will only provide data specific to one unique trace number. Now the user will see the true response from a single request without any additional elements from other transactions.

7. This patch will remove the corrupted records that currently exist in the INSURANCE VERIFICATION PROCESSOR File (#355.33).

This patch also addresses two defect tracking system tickets:

Ticket INC9335636 (Same as Rational Defect #1217953)

Problem: When users try to transmit claims using the ^RCB option, users are kicked out of VistA upon submitting the claim.

Resolution: Modified routine IBCEPTC to revert a FileMan screening logic to return to the original code; thus, undoing the modification that was introduced with IB*2.0*623. This error resulted in kicking users out of VistA. This problem is restricted to the Region 1 sites and a few that are in the cloud. This corrects the <PROTECT> error that the users encountered when they used the VistA option VIEW/RESUBMIT CLAIMS - LIVE OR TEST [IBCE PREV TRANSMITTED CLAIMS] and selected to transmit by claim number.

Ticket INC9338421

Problem: I get an error saying SORRY 'BOUT THAT $ ZERROR

Resolution: Modified routine IBCE by removing a line of code that was introduced with IB*2.0*623 that triggered a <SYNTAX>DIE+8^DIE error. This error resulted in kicking the user out of VistA. This occurred when the user was in the VistA option CLAIMS STATUS AWAITING [IBCE CLAIMS STATUS AWAITING] and selected the action to 'Retransmit'.

5.3 Back-Out Criteria

The project is canceled, or the requested changes implemented by IB*2.0*659 are no longer desired by VA OI&T and the eBusiness eInsurance sub-team, or the patch produces catastrophic problems.

5.4 Back-Out Risks

Since the eInsurance software is tightly integrated with external systems, any attempt at a back-out should include close consultation with the external trading partners such as the Financial Services Center (FSC) and the Health Care Clearing House (HCCH) to determine risk.

5.5 Authority for Back-Out

Any back-out decision should be a joint decision of the Business Owner (or their representative) and the Program Manager with input from the Health Services Portfolio (HSP) Application Coordinator, developers (both project and Tier 3 HSP), and if appropriate, external trading partners such as the VA Financial Service Center (FSC) or Health Care Clearing House.

eInsurance is tightly integrated with these external partners and a back-out of the patch should not be a standalone decision.

5.6 Back-Out Procedure

The back-out plan for VistA applications is complex and not a "one size fits all" solution. The general strategy for a VistA back-out is to repair the code with a follow-up patch. The development team recommends that sites log a ticket if it is a nationally released patch.

Back-Out Procedure prior to National Release. If it is prior to national release, the site will be already working directly with the development team daily and should contact that team. The development team members will have been identified in the Initial Operating Capability (IOC) Memorandum of Understanding (MOU). As discussed in section 5.2, it is likely that development team can quickly address via a new software version. If the site is unsure who to contact they may log a ticket of contact Health Services Portfolio - Management Systems Team.

The IB*2.0*659 patch contains the following build components.

- Data Dictionary
- Enhancements
- Routines

While the VistA installation procedure of the KIDS build allows the installer to back up the modified routines using the 'Backup a Transport Global' action, due to the complexity of this patch, it is not recommended for back-out, and a restore from a backup of the Transport Global should not be attempted. In the event that a site decides to back out this patch, the site should contact the Enterprise Service Desk (ESD) to submit a help desk ticket. The development team will need to issue a follow-on patch in order to comprehensively back-out this patch and/or to clean up corrupted data/remove data dictionary changes, if needed and restore the system to a functioning state.

Please contact the EPMD team for assistance since this installed patch contains components in addition to routines.

5.7 Back-out Verification Procedure

Successful back-out is confirmed by verification that the back-out patch was successfully implemented. This includes successful installation and testing that the back-out acted as expected, as defined together with the team the site contacted in section 5.5.

6 Rollback Procedure

Rollback pertains to data. The only data changes in this patch are specific to the operational software and platform settings and they are covered in the Back-out procedures detailed elsewhere in this document.

6.1 Rollback Considerations

Not applicable.

6.2 Rollback Criteria

Not applicable.

6.3 Rollback Risks

Not applicable.

6.4 Authority for Rollback

Not applicable.

6.5 Rollback Procedure

Not applicable.

6.6 Rollback Verification Procedure

Not applicable.

Template Revision History

Date	Version	Description	Author
March 2016	2.2	Changed the title from Installation, Back-Out, and Rollback Guide to Deployment and Installation Guide, with the understanding that Back-Out and Rollback belong with Installation.	VIP Team
February 2016	2.1	Changed title from Installation, Back-Out, and Rollback Plan to Installation, Back-Out, and Rollback Guide as recommended by OI&T Documentation Standards Committee	OI&T Documentation Standards Committee
December 2015	2.0	The OI&T Documentation Standards Committee merged the existing *"Installation, Back-Out, Rollback Plan"* template with the content requirements in the OI&T End-user Documentation Standards for a more comprehensive Installation Plan.	OI&T Documentation Standards Committee
February 2015	1.0	Initial Draft	Lifecycle and Release Management